Addressing heterogeneity in model-based development of cyber-physical systems

Akshay Rajhans

ECE PhD candidate, Carnegie Mellon University

arajhans@ece.cmu.edu
http://users.ece.cmu.edu/~arajhans

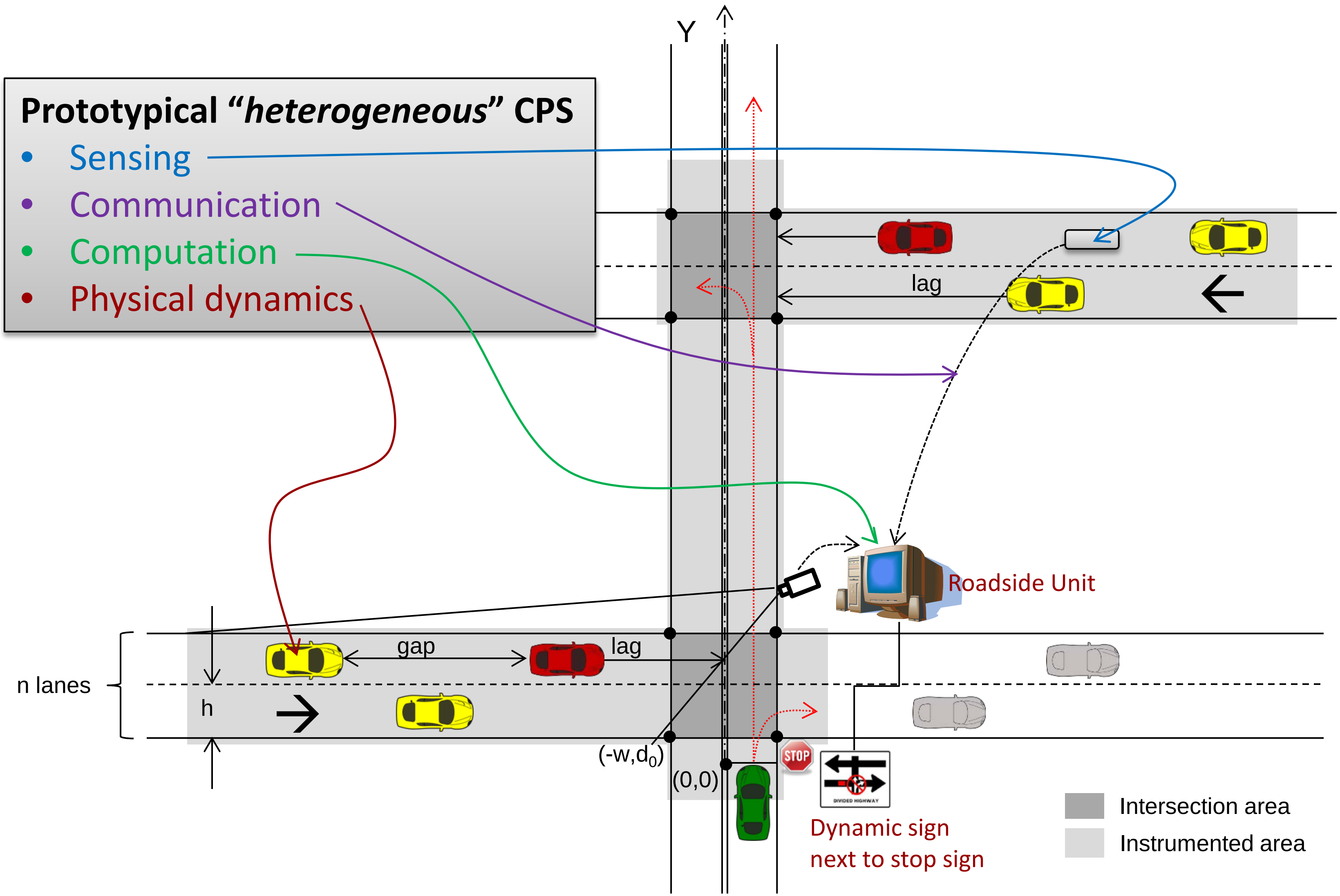
Joint work with
Ajinkya Bhave, Bruce Krogh, David Garlan, Sarah Loos, Andre Platzer, Ivan Ruchkin, Bradley Schmerl
ECE Department, School of Computer Science, Carnegie Mellon University

Electrical & Computer ENGINEERING

CPS are *heterogeneous*

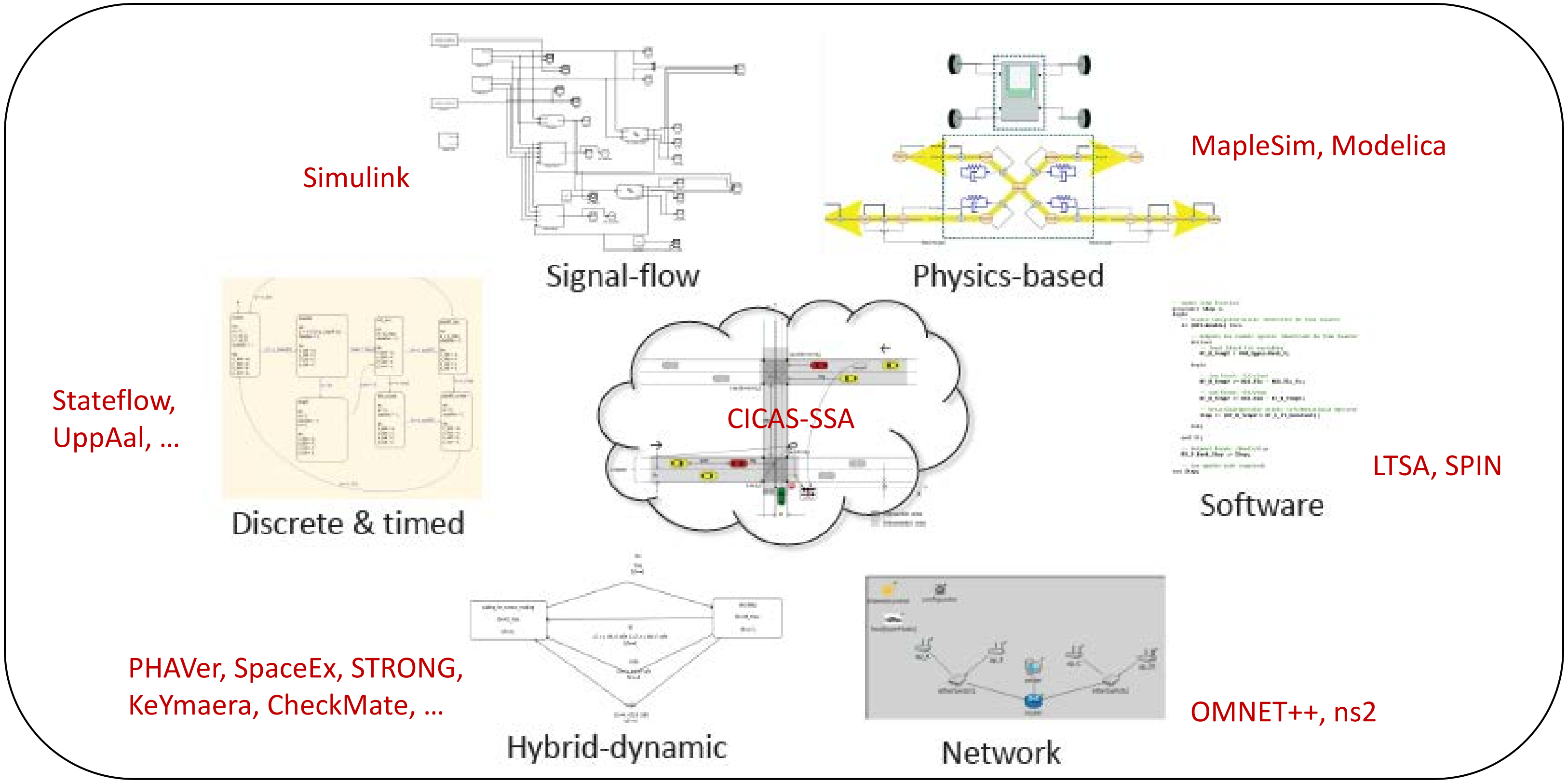
Example: CICAS-SSA*

Prototypical "*heterogeneous*" CPS
- Sensing
- Communication
- Computation
- Physical dynamics



*Cooperative Intersection Collision Avoidance System for Stop-Sign Assist

Heterogeneity in Models & Analysis Tools

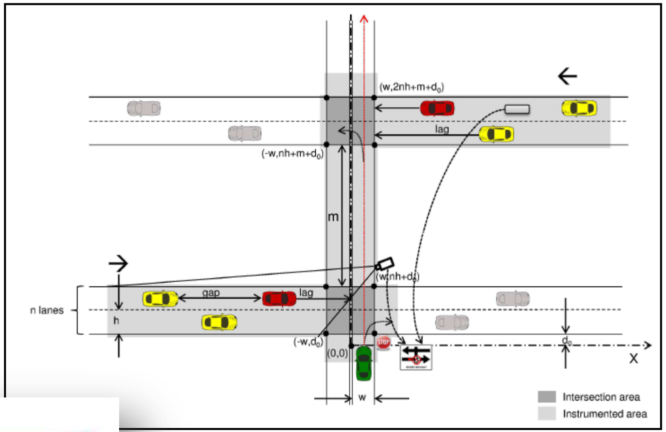


Challenges:

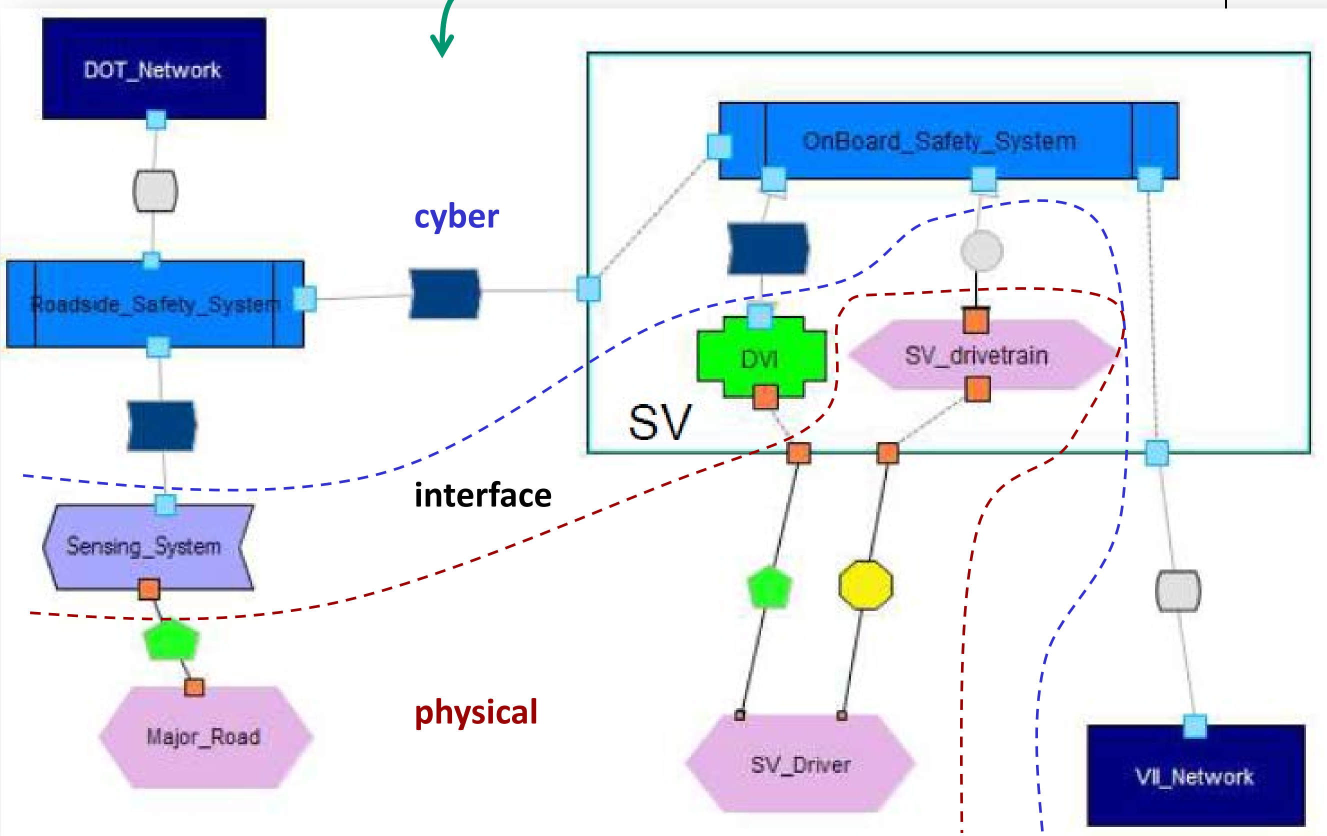
- *No "universal" modeling formalism* that can capture everything.
- Each model represents *some* design aspect well, but not the others.
- Models make *(interdependent) simplifying assumptions*.
- Different *tools* leverage different properties, *work only with their formalism*.

How do we ensure correctness of the system without a unifying formalism?

Architectural Modeling of CICAS



CICAS: Architectural modeling depicting interacting run-time components and connectors



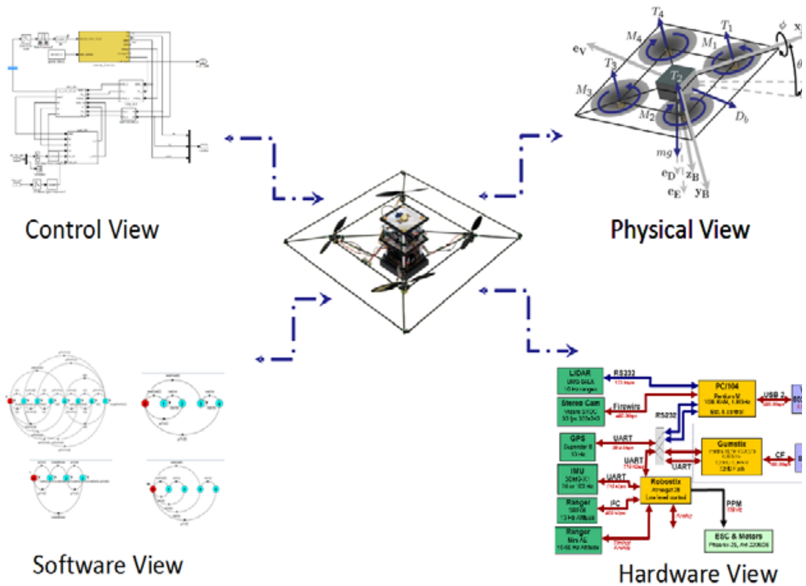
CICAS: Actual System

– *Visual representation with unambiguous* (but very basic) *semantics*

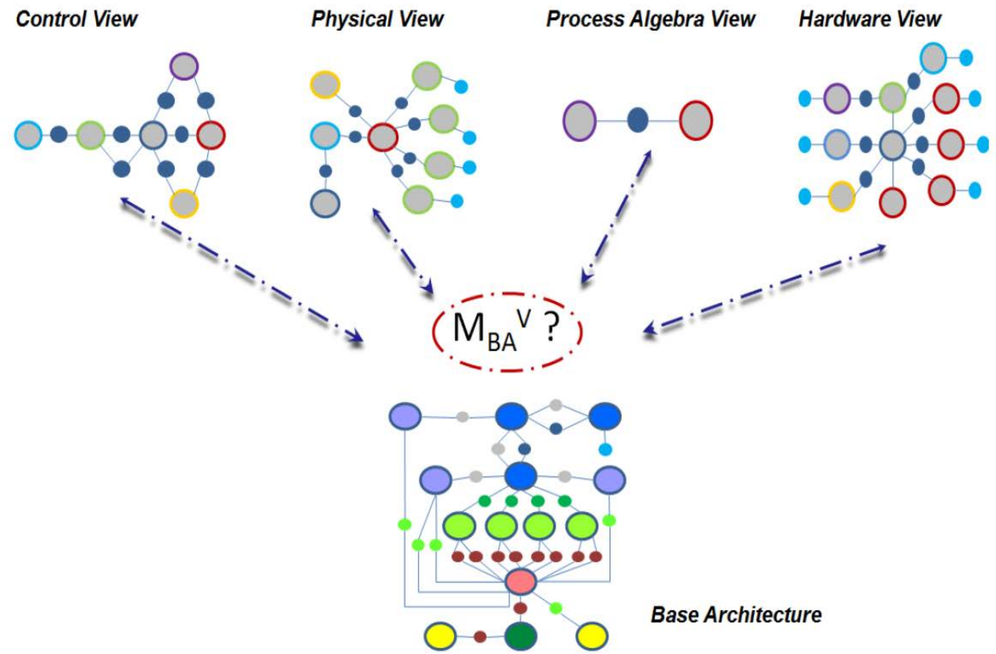
(no behavior info.)

Heterogeneous models as arch. views

Example: STARMAC quadrotor



Models as architectural views



Structural consistency using graph morphisms

Augmenting Software Architectures with Physical Components

Ajinkya Bhave[1], David Garlan[2], Bruce H. Krogh[1], Akshay Rajhans[1], Bradley Schmerl[2]
[1]Dept. of Electrical and Computer Engineering
[2]School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3890 USA
email: {ajinkya@ | garlan@cs.| krogh@ece.| arajhans@ece.| schmerl@cs.}cmu.edu

ERTS² '10

View Consistency in Architectures for Cyber-Physical Systems

ICCPS '11

Ajinkya Bhave, Bruce H. Krogh David Garlan, Bradley Schmerl

Ensures consistent functional deployment in model subcomponents

Electrical & Computer ENGINEERING

★ Heterogeneous abstraction/implication

1. Define *behavior relations* R_i between abstract domains B_i and detailed domain B_0

2. Extend notions of abstraction/implication to heterogeneous domains via these R_i

Heterogeneous Abstraction

$M_0 \sqsubseteq^{R_1} M_1$, if (behavior set overapproximation via R_1)

$$[\![M_0]\!]^{B_0} \subseteq R_1^{-1}([\![M_1]\!]^{B_1}).$$ A

Heterogeneous Specification Implication

$S_1 \Rightarrow^{R_1} S_0$, if (behavior set underapproximation via R_1)

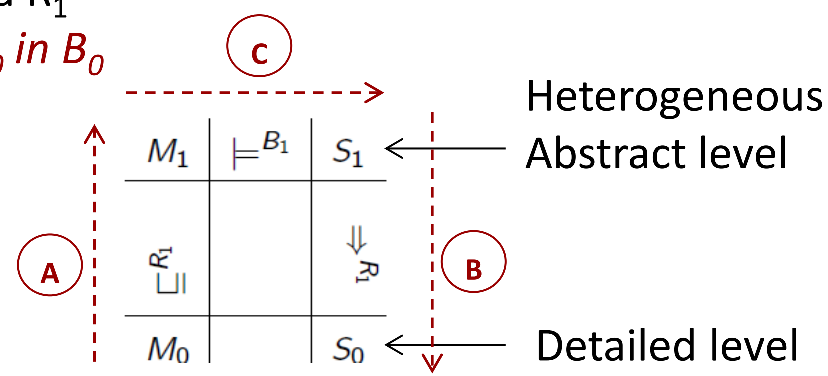
$$R_1^{-1}([\![S_1]\!]^{B_1}) \subseteq [\![S_0]\!]^{B_0}.$$ B

3. If *M_1 abstracts M_0* and *S_1 stronger than S_0* via R_1
then *M_1 satisfies S_1 in B_1* implies *M_0 satisfies S_0 in B_0*

Heterogeneous Verification

If $M_0 \sqsubseteq^{R_1} M_1$, $M_1 \models^{B_1} S_1$ and $S_1 \Rightarrow^{R_1} S_0$, then $M_0 \models^{B_0} S_0$. C

(in words)



(pictorially)

Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

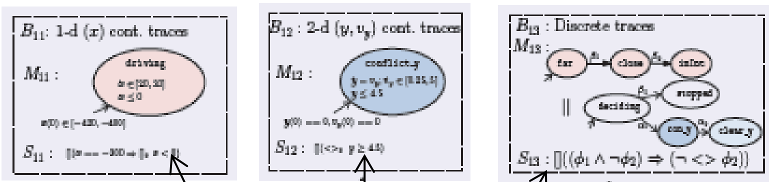
HSCC '12

Akshay Rajhans
arajhans@ece.cmu.edu

Bruce H. Krogh
krogh@ece.cmu.edu

★ Enables heterogeneous verification

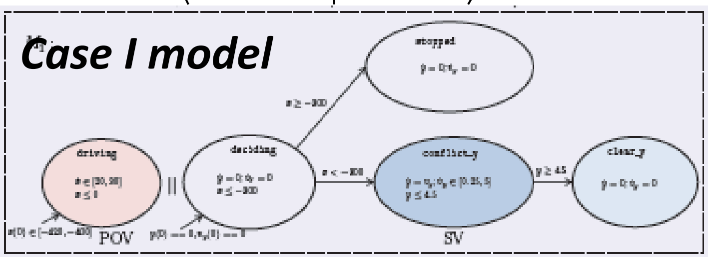
Hierarchical heterogeneous verification of CICAS-SSA



...

Conjunctive breakdowns
- M_{1i} individually cover M_1
- S_{1i} together imply S_1

Case I model



No right turn

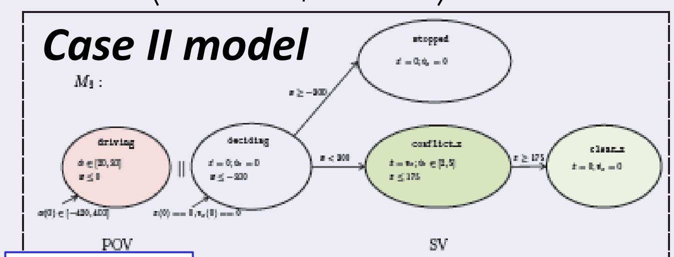
B_1 : 3-d ($\{x, y, v_y\}$) hybrid traces

$S_1 : \Box \neg (x == 0 \wedge 0 < y < 4.5)$

R_1: equal values along x, y, v_y; z, v_z zero over all time

$R_1^{-1}([\![S_1]\!]^{B_1}) : \Box ((\neg(x == 0 \wedge 0 < y < 4.5)) \wedge (z == 0 \wedge v_z == 0))$

Case II model



No straight crossing

B_2 : 3-d ($\{x, z, v_z\}$) hybrid traces

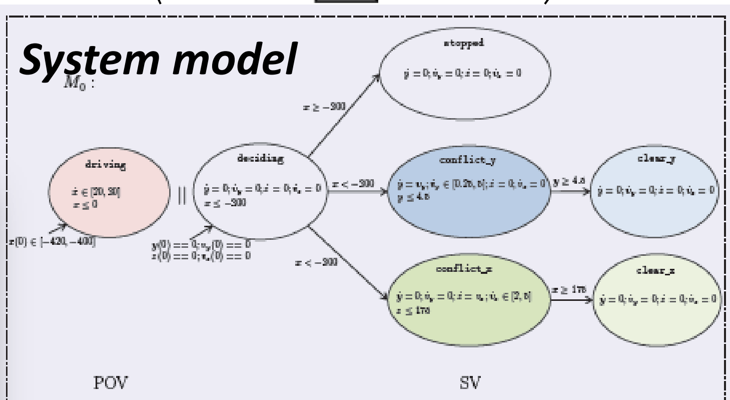
$S_2 : \Box \neg (x == 0 \wedge 0 < z < 170)$

R_2: equal values along x, z, v_z; y, v_y zero over all time

$R_2^{-1}([\![S_2]\!]^{B_2}) : \Box ((\neg(x == 0 \wedge 0 < z < 170)) \wedge (y == 0 \wedge v_y == 0))$

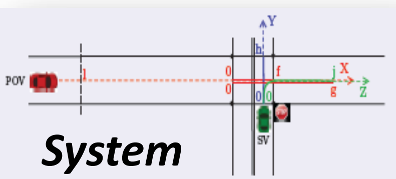
Disjunctive breakdown
- M_i together cover M_0
- S_i individually imply S_0

System model



B_0 : 5-d ($\{x, y, v_y, z, v_z\}$) hybrid traces

$S_0 : \Box \neg ((x == 0 \wedge 0 < y < 4.5) \vee (x == 0 \wedge 0 < z < 170))$

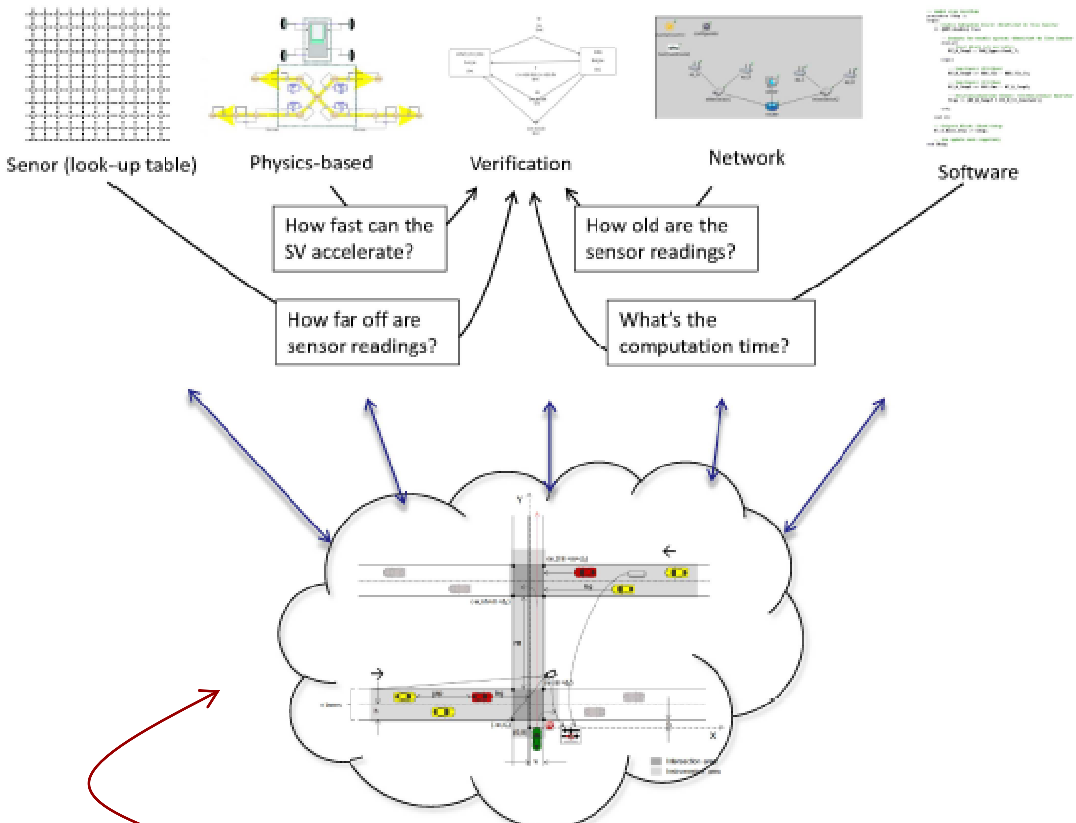


System

A simple CICAS-SSA with one highway lane and one oncoming vehicle.

5-d hybrid verification simplified to *1-d, 2-d continuous* and *discrete* verifications

Semantic assumptions as parameter constraints



Dependencies that cut across modeling formalisms can be captured as parameter constraints

Problem

- Semantic interdependencies cut across modeling formalisms.
- Consistency needs to be ensured to guarantee system verification.

Challenge

- Interdependencies need to be formally represented
- Representation needs to be universal to all modeling formalisms

Approach

- Identify model and spec. parameters explicitly
- Model interdependencies as an *auxiliary constraint*
- Find *effective constraint* on given model/spec. parameters using projection (existential quantification)
- Prove consistency in SMT solvers or theorem provers

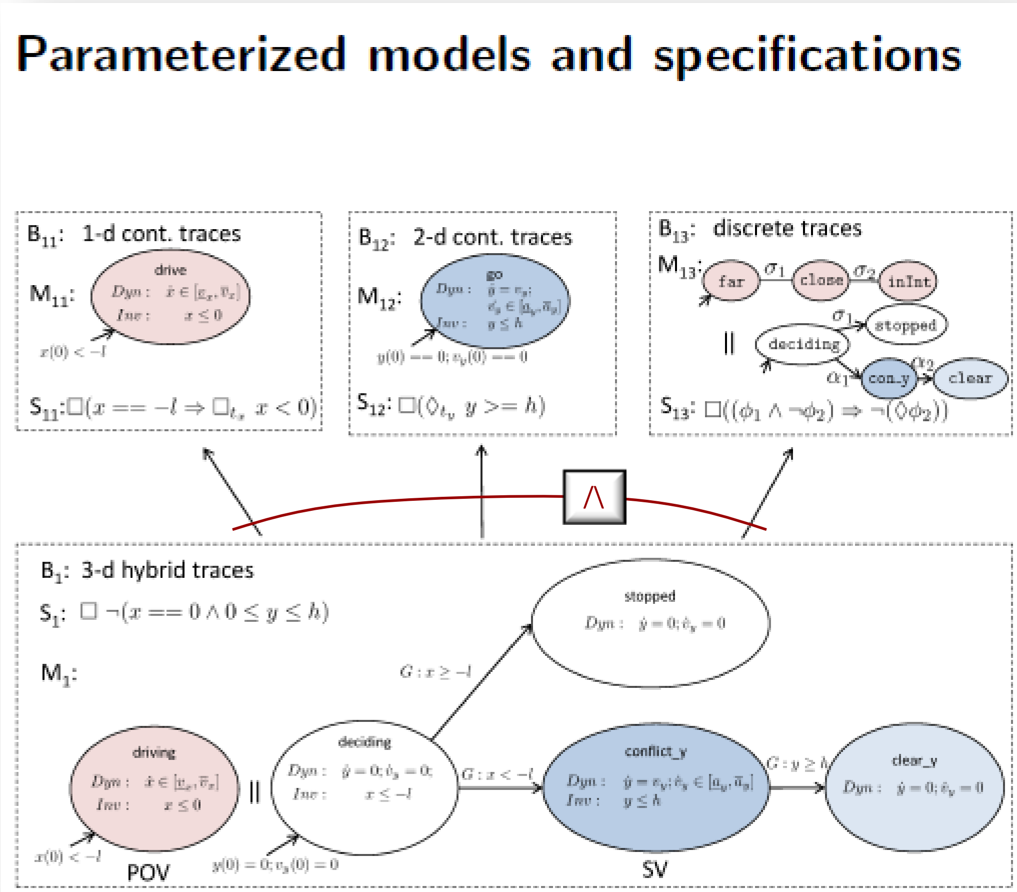
CDC '11

Using Parameters in Architectural Views to Support Heterogeneous Design and Verification

Akshay Rajhans†, Ajinkya Bhave†, Sarah Loos‡, Bruce H. Krogh†, André Platzer‡, David Garlan‡

Ensures semantic (parameter) consistency using external SMT solvers or provers

⭐ Parametric verification of CICAS



Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

HSCC '12

Akshay Rajhans
arajhans@ece.cmu.edu

Bruce H. Krogh
krogh@ece.cmu.edu

1. Explicitly identify model parameters e.g. *speed limits, intersection geometry, minimum acceleration,* and *spec. parameters*, e.g., *POV min. time-to-intersection, SV max. time-to-clear-intersection*

2. Model interdependencies as an auxiliary constraint
e.g., those dictated by *speed limits, newton's laws* and *intersection geometry* on *time-to-intersection*, …

3. Project global constraints and interdependencies (aux. constraint) onto local sets of parameters

⭐ Proved semantic consistency in theorem prover KeYmaera